nSA Release Notes

22.8R1.2

Copyright Notice

Contents

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
3.4	April 2025	22.8R1.2 release notes. Updated the following topics: • "What's New" on page 6 • "Resolved Issues" on page 18 • "Known Issues" on page 32
3.3	February 2025	22.8R1.1 release notes. Updated the following topics: • "Supported and Compatibility " on page 15 • "Resolved Issues" on page 18
3.2	January 2025	22.8R1 release notes. Updated the following topics: • "What's New" on page 6 • "Limitations" on page 48 • "Supported and Compatibility " on page 15 • "Resolved Issues" on page 18
3.1	January 2025	Updated the 22.7R2.5 package upgrade links. "Supported and Compatibility " on page 15
3.0	November 2024	22.7R1.6 release notes
2.9	October 2024	22.7R1.5 release notes
2.8	September 2024	Updated the 22.7R2.2 package upgrade links. "Supported and Compatibility " on page 15
2.7	August 2024	22.7R1.4 release notes
2.6	July 2024	22.7R1.3 release notes. Updated the following topics:

Revision	Revision Date	Description
		• "What's New" on the next page • "Limitations" on page 48 • "Supported and Compatibility " on page 15 • "Resolved Issues" on page 18 • "Resolved Issues" on page 18
2.5	July 2024	22.7R1.2 -HF3 release notes updates
2.4	May 2024	22.7R1.2 release notes
2.3	April 2024	Resolved Issues list is updated for 22.7R1
2.2	March 2024	22.7R1 release notes
2.1	February 2024	22.6R1.7 release notes
2.0	February 2024	22.6R1.6 release notes
1.9	January 2024	22.6R1.5 release notes
1.8	October 2023	22.6R1 release notes created
1.7	July 2023	22.5R1 release notes created
1.6	June 2023	22.4R3 release notes created
1.5	April 2023	22.4R1 release notes created
1.4	November 2022	22.3R1 release notes created
1.3	July 2022	22.2R1 release notes created
1.2	April 2022	22.1R1 release notes created
1.1	January 2022	21.12 release notes created
1.0	October 2021	21.9 release notes created

What's New

22.8R1.2

- **Gateway Upgrade Improvements**: nSA now provides option to stage the package on individual Gateway/Cluster or multiple Gateways/Clusters, and upgrade the Gateways manually or on a specified date and time. The Gateway stage and upgrade is supported from ICS Gateway 22.7R2.8 release. For more details, see Upgrading Gateways and Clusters with a New Gateway Version.

This capability is available from ICS Gateway 22.7R2.8 version onwards.

- **nSA Syslog Server Integration**: nSA enables you to configure external syslog server to forward ICS Gateway logs and nSA Tenant Admin logs. This enables centralized and secure log management and enhanced visibility into the health and efficiency of the services running in your ICS Gateways, or to facilitate debugging in the event of unexpected service behavior. For details, see Using Enterprise Integration to Export Your Logs for External Analysis.
- **Config Sync Enhancements**: Config Sync enhancement supports configuring the entire configuration synchronization across multiple targets (up to 15 targets for entire configuration and 50 targets for selective configuration). This enhancement enhances flexibility and scalability for managing multiple gateways or clusters. This is particularly useful for enterprises with extensive networks, as it simplifies configuration management across various systems. This feature is supported from ICS Gateway 22.7R2.8 release. For details, see Config Synchronization.
- **Segregation of app visibility logs**: In order to avoid performance issue, app visibility logs is segregated from user access logs. App visibility logs is available in debug log/snapshot for troubleshooting. This feature is supported from ICS Gateway 22.7R2.8 release. For details, see Using the Debug Log.
  The maximum debug log file size for Gateways with disk space > 80 GB is increased to 1024 MB.
- **Reporting Enhancements**:
  - The number of schedule/on-demand exports is increased to 10.
  - Summary charts of gateways, user roles, application access, anomalies, non-compliance, and user risk now displays top 100 with more than 1 lakh users aggregation.
  - User analytics now shows maximum top 30 users.
- **Admin experience enhancements**:

- Search and Sort options are added for selective tables:
  - Gateway > Users > Resource Policies
  - Gateway > System > Configuration, Network, IF-MAP Federation, Log/Monitoring
  - Gateway > Authentication > Signing In, Authentication Servers

Move Up and Down arrow option is disabled when Search function is applied to a table.

- **Feature Parity with ICS Gateway**:
  - For Gateways with disk space > 80 GB, maximum debug log file size is increased to 1024 MB. For details, see Using the Debug Log. This change is applicable from ICS 22.7R2.6.
  - VPN Tunneling Resource Policy configuration allows you to enable / disable IPv4 and IPv6 address assignments and specify IPv4 and IPv6 address ranges. For details, see VPN Tunneling Resource Policy Configuration Use Case. This change is applicable from ICS 22.7R2.6.

22.8R1.1

This release includes bug fixes. There are no new features.

22.8R1

- **Enhancements to Tenant Admin Audit Logs for end-to-end admin activities**: Tenant Admin logs now captures all the admin activities from login to logout. For more details, see Checking Tenant Admin Logs.
- **Config Sync enhancements**: Admin can now schedule config sync rule jobs to run only on a specified time or to run daily, weekly or monthly frequencies. For more details, see Scheduling Config Sync Rule Job.
- **Admin experience enhancements**: Search and Sort options are added for tables in Gateway > Users > Roles, Realms, and Resource Profiles, and Authentication > Endpoint Security.
- nSA Config Authoring can handle multiple certificates with the same serial number.

22.7R1.6

- **(Preview) Enhancements Tenant Admin Audit Logs for Gateway operations**:Tenant Admin Logs page now additionally shows the audit logs generated for config change operations (create/update/delete) performed by all admins. For more details, see Checking Tenant Admin Logs.
- **Config Sync enhancements**: "Duplicate Config" option is newly added in the Config Synchronization Status page to clone the config sync rule. For more details, see Cloning a Config Sync Rule.
- **Admin experience enhancements**: "Group by" option is added in the Gateway List page to filter the list based on Gateway Type, Connection status, Version or Region.

22.7R1.5

- **(Preview) Tenant Admin Audit Logs for Gateway operations**: Tenant Admin Logs page is newly added to show nSA admin audit logs generated for Gateway operations such as create, delete, upgrade, reboot and rollback. For more details, see Checking Tenant Admin Logs.
- **Password policy for XML configuration export and import, and TOTP users export and import**:
    - Strengthening the XML configuration file import/export process with password authentication checks. For more details, see: Exporting an XML Configuration File.
    - Strengthening the TOTP server by adding password authentication checks for importing and exporting the users data file. For more details, see: Exporting/Importing TOTP Users.
- **Config Sync enhancements**: "Refresh Gateway Status" option is newly added in Config Synchronization Status page for target gateways with status "Pending", "Importing" or "Timed out". For more details, see Config Synchronization.
- **Admin experience enhancements**:
    - Alphabetical sorting (ascending / descending) is now possible in the Gateways List and the Config Synchronization pages. Use the arrow icon provided in the column header to show alphabetically sorted list.
    - "Expand all / Collapse all" functionality is added in the Gateways List page. Use the Expand all / Collapse all icon provided in the Gateways List page to expand / collapse the Clusters and Gateways lists.

22.7R1.4

- **Admin UI user experience enhancements**: Column reordering is newly added in the Users L3 and L4 pages. To move a column, a user can click the header and drag to its new position. For more details, see Ivanti Connect Secure Gateway Analytics.

22.7R1.3

- **Consolidated landing page**: Drill down support for the Sankey chart is newly added on the consolidated landing page. With each chart, the View all link provides a page with detailed log records for that category. For more details, see Consolidated Landing Page, see Consolidated Landing Page.
- **Multinode configuration status enhancement**: configuration status now includes start and end timestamps and additional status information. For more details, see Config Synchronization.
- **All Gateways Counter**: All Gateways counter is newly added on ZTA and nSA specific analytics landing page. For more details, see Reviewing Your Network Activity. For more details, see Registering Ivanti Connect Secure Gateway and Creating an ICS Cluster.
- **Gateway name / Cluster name length**: The maximum length of ICS Gateway name / Cluster name is increased to 19 characters. Admin can now register the existing ICS Gateway Cluster with cluster name length up to 19 characters to nSA.
- **Feature parity with ICS Gateway 22.7R2.1 version**:
  - Max log Size for Event logs: The range is 1- 200 MB and the maximum size is 200 MB for Virtual Appliances. The range is 1- 1024 MB and the maximum is 1GB/1024MB for ISA Hardware. For details, see Events to Log.
  - Play integrity check for rooting detection on Android devices: checks if interactions and server requests are coming from the genuine app binary running on a genuine Android device. For details, see Mobile Configuration.

22.7R1.2

- **(Preview) Consolidated landing page**: A new unified landing page allows tenant admin to examine the shared analytical tables and charts for nZTA and ICS Gateways. For more details, see Consolidated Landing Page.

- **Admin UI user experience enhancements**: Improvements to the admin experience (Modernize the table view for session management and log view). Advanced filter on the page for managed users. For more details, see:
  - Checking the Logs
  - Managing the Sessions
  - Viewing Admin Authentication Methods
  - Viewing Admin Authentication Policies
  - Creating Admin Groups
- **Sync Now**: A new Sync Now page allows the tenant admin to implement changes made to Admin Management and correct any configuration problems based on the alerts. For more details, see Synchronizing the Configuration.

22.7R1

- **Admin Experience Enhancements**: To enhance the administrative experience, there have been improvements in the form of table modernization for both Admin Management and Session Management. For details, see nSA Administration.
- **Password Strengthening for Local Authentication Server**: The local authentication server has stronger password restrictions. For details, see Workflow: Creating a Local Authentication Policy.

22.6R1

- **IPv6 L3 VPN Application Visibility** (Supported only for 22.x ICS Gateway): Support for IPV6 L3 VPN visibility in nSA. You can view both IPv4 and IPv6 applications for L3 user sessions from the Applications overview page. For details, see Using the Applications Filter Bar.
- **nSA Named User License Normalization** (Supported only for 22.6R2 ICS Gateway with 22.6R1 ISAC Client and later versions): Normalization of license seat reservation across devices and users. Single license is consumed instead of two through associating devices with users for Machine Cert Authentication and subsequent User Authentication. For details, see nSA Licensing/Subscription.
- **Licensing Enhancements for named user licenses (UAL)**: Support added to perform out of band license checks. The subscription page in nSA tenant admin portal will be updated with few minutes of delay from the new user login.

- **nSA Feature parity with 22.6R2 ICS gateway**
  - Resource policies > VPN Tunnelling > Connection Profile > DHCP Subnet - 22.x
  - HTML5 Bookmark - Enable Auto Resolution Option - 22.x and 9.x
  - User Roles Options - Enable Auto Resolution Option - 22.x and 9.x
  - System > Configuration > SAML > New SAML > Hide PDP Option - 22.x
  - Hide Authentication > Auth Servers > LDAP server > Health check - 9.x
  - Authentication > Auth Servers > LDAP server > Health check - 22.x
  - System > Configuration > Security > Miscellaneous > Relay state option - 22.x
- **Support SAML Authentication server as a secondary authentication server when configuring Certificate Authentication server** (Supported only for 22.x ICS Gateway): nSA now supports configuration of Certification Authentication server with SAML Authentication server as a secondary authentication server. For details, see Configuring Certificate Authentication Server.
- Admin experience enhancements to L4, Gateway Logs, and Logs Tables in terms of selection and resizing, pagination, and text copy/paste

  The following list shows the enhancements to L4, Gateway Logs, and Logs Tables.
  - Column resizing across ICS pages
  - Cell content copy text from Table
  - Pagination across ICS pages
  - Minimum number of columns in all the tables in L4 dashboards
  - Enhancement to Advanced Filter

For details, see Using the Top Active Breakdown Charts and Filtering the Logs.

22.5R1

- **Auto Selecting Dependent Configurations as part of Config Sync**: While creating config sync rule, if there is any dependency mismatch, admin can review dependent configurations and select them before creating/editing rule. For details, see Config Synchronization.

For example, If realm configuration is mapped to Authentication server and if config sync rule is created with only realm. The dependent configuration is highlighted (Auth server). Realm configuration is highlighted with i icon and when dependencies are reviewed, Authentication server is mentioned in the dependency tree.

- Preview of changes done in source gateway before config sync. This feature is available only with Manual sync.

Preview before sync will work only when one manual config sync rule is triggered.

- 22.5R2 ICS configuration parity in nSA.
- **Admin Access Control based on location, Host Checker, and Network**: Checks the Admin's device geographic location/network/host checker compliance for admin sign-in policy before providing access to admin login. For details, see Creating Admin Policies.
- **nSA Licensing Enhancements**: When nSA licensing is enabled on Gateway, and if there is connectivity issue between gateway and controller, grace period of 24 hours is applied for new user logins up to platform limit.

22.4R3

- **Role Based Access Control for Admin Users**: With Role-based access control (RBAC), organizations can easily add admins and assign them specific roles, with differing levels of access to the nSA Admin Portal. In addition to an existing set of default roles, Administrators can now create custom granular roles for specific functions within the nSA admin portal. For details, see Role-based Access Control for Admin Users

22.4R1

- **Analytics: Historical View**: Analytics supports data visualization in Active View. Admin can see the historic data on different time windows. Admin's can find all connections details for different time frames past 30 days. For details, see Using the Filter Bar
- **Config Sync Rule Status**: This feature allows a user to view the config sync rule status of all target gateways. For details, see Config Synchronization.

- **nSA named user licensing normalization**: This feature allows a user to use different login formats - Domain\username, Common Name (CN), and User Principal Name (UPN) - from different devices, but consumes only one seat for the user. For details, see nSA Licensing/Subscription.

22.3R4

- **Configuring ZTA Policy to an ICS Application**: Administrators can now configure ICS application with ZTA secure access policy from the nSA-ICS Applications page.
- **nSA Named User Licensing - Freeing named user licenses automatically**: Users who have not logged in to the ICS Gateway for the last 30 days can be deleted automatically from the Users list.
- **Addition of a new alert "Config Sync Target Cluster Deleted**": This alert is generated when the Target Cluster, which is in any of the Config Sync rule gets deleted.

Configuration template functionality is consolidated into Configuration sync feature.

22.3R3

Actionable Insights: Step up Authentication, Subsequent login and Chart Visibility.

22.3R1

- Enhanced Admin experience
- Config Sync enhancements
- Alerts and Notification enhancements
- nSA UI parity with 9.1R16 and R17
- L3 VPN App Visibility
- Config Replace/reorder

Introduction

If the information in these Release Notes differs from the information found in the online documentation, refer to the Release Notes as the source of the most accurate information.

The information in this Release Notes relates to the following releases:

- nSA 22.8R1.2
- nSA-managed ICS 22.7R2.7 Build 4377

References

• For resolved issues in the ICS 22.x Gateway, refer the Release Notes

Supported and Compatibility

Download the ICS Gateway image and template files from the Software Download Portal.

Release and Upgrade Notes

Important Notice for v22.3R1 and Later

To prevent any upgrade related issues and to clean up the disk space, follow the mandatory steps listed in the KB article before staging or upgrading: KB.

Important Notice for v22.1R1 and Later

nSA 22.1R1 includes updates to address the OpenSSL vulnerability described in CVE-2022-0778. Ivanti recommends upgrading your Gateways to version 22.1R1 at your earliest convenience.

Caveats

The following caveats are applicable to this release:

- Analytics Dashboard and Gateway logs are not synchronized with nSA when using an ICS gateway on the cloud running version 22.5R2 or above.
- Gateway ESAP package version 4.3.8 is default.
- Config group management works best with ESAP version 4.0.5. The ESAP version on the Gateway can be upgraded to desired version.
- For uploading the ESAP package, you must have the package in ESAP<version>_Prod.pkg format.
- Config Synchronization feature:
    - Active ESAP versions must be same on both Source and Target Gateways.
    - Admin Realms, Admin Sign-In URLs, Device certificates and Client Auth certificates are not supported.
    - During Config Synchronization, the configurations will be getting merged from Source Gateway to Target Gateway and hence the delete operation is not supported.
- nSA accepts only certificates in PEM format, DER format certificates are not supported from nSA.
- nSA custom validation is not supported through Configuration Templates. The UI may accept invalid configuration parameters.

- Remote profiler and OAuth server are not supported through Configuration templates.
- Always on VPN wizard is not supported on nSA.
- Dark theme for nSA ICS admin UI is not supported.
- ICS Cluster creation with IPv6 address from nSA is not supported.

Additional Notes

Rollback - When we rollback to previous versions of 9.1Rx (where nSA is not supported), the status in nSA shows disconnected.

Resolved Issues

The following table describes the issues resolved.

Problem Report	Description
22.8R1.2	
1537020 1532564	Configuration Sync is now enhanced to resolve the issues with the entire Config Sync with multiple targets (upto15 targets).
1532636	The issue with Inaccurate active user session information on nSA controller is resolved.
1525136	Schedule Log export fails to generate an export (CSV/JSON) if it scheduled for a week.
1516701	The Date format on the X axis in "Overall Concurrent-Users License Usage" when navigating under Insights > Gateways now shows the desired values.
1525838	Compatibility issue during selective config sync operations between source gateways running version 22.7R2.5 (or lower) and target gateways running version 22.7R2.6 is resolved.
1479451	Custom ESAP package: Uploading the same version of an ESAP package, which is already present as a custom package triggers an error in the UI.
1479527	The validation for wrong package upload is added.
22.8R1.1	
1505663	The intermittent issue of nSA license users not appearing on the users page in the nSA controller has been resolved.
1476344	With nSA license, few users are not reflecting in users page in the controller.
22.8R1	

Problem Report	Description
1416167	The incorrect readiness failure logs observed due to legitimate disconnections, such as the 24-hour disconnect is now fixed.
1430129	The mismatch between SessionCreated and Logout messages on the nSA controller has been fixed.
1478099	The issue with the Home Page incorrectly displaying statistics for the top users' count by gateways has been resolved
1473136	The issue with acknowledging all anomalies under the Overview Page has been resolved.
1487582	The administrator name now appears fully on the landing page.
1473258	The Config Sync status error is resolved.
22.7R1.5	
1447143	The issue with the active users information not shown in the nSA license subscription page is now resolved.
22.7R1.4.2	
1422086	The config sync rule execution is fixed by increasing the memory size.
1422579	The Auto-Delete setting values are now retained while using filters, switching between tabs, and returning to the Users tab.
22.7R1.4	
1393303	Config sync is failing with error Missing root or parent certificate. Trusted Client CAs > Trusted Client CA.
1385665	User login issues when nSA connectivity is lost on ICS 22.7R2 despite the 24 Hour Grace Period.

Problem Report	Description
1394450	nSA - Users are unable to fetch the License from the nSA.
1395150	UAL license not working for EU region.
1391196	Username sorting is not working on Subscriptions > Users page.
1391819	Any number of nodes can be added while creating cluster from nSA.
1384267	nSA will allow to add any number of nodes to the cluster with hardware devices while it is restricted to 2 nodes for virtual(ISA-V) gateways registered to controller
22.7R1.3	
1341772	Sankey chart does not show the exact path for application being accessed with respect to usergroup.
1371046	UEBA threat score showing - Request Failed with status code - 500.
1375846	Unable to Acknowledge all active anomalies under Overview Page.
1378162	Overview Page should display all the Gateways registered with the controller.
1378578	nSA Subscription count is showing over consumption with only 25K users and remaining 50K from devices.
1378134	Fixed issue with Config Synchronization.
1372365	Read-Only Mode not working while using Cluster on the nSA.
1364287	Latest Logs are not populating properly in the nSA even though the ISA device has the latest logs available.

Problem Report	Description
1373268	Cluster Name Limitations in nSA and ICS.
1350471	Auto-Delete of users failing in Controller after 30 days of inactivity
1350344	Push config - job status pending, but the logs on the gateway indicate that it has already been completed.
1350345	Config sync logs gets automatically removed from nSA.
1350442	Gateway Configuration tasks from controller are stuck in pending state.
1377012	Ivanti Neurons admin policies are displaying "No data SAML metadata."
1371037	Intermediate Certificate of clustered gateway not loading on the nSA.
1371041	Misleading Active Gateway details on the Network Overview page.
1371044	The gateway overview page is not showing correct data about the Gateway Versions count.
1350424	Unable to import trusted client CA to nSA, while gateway accepts same certificate.
22.7R1.2-HF3	
1369055	Pushing the configuration from nSA caused changes to the split tunneling settings.
1371037	The nSA is unable to load the intermediate certificate for the clustered gateway.
1372365	Read-Only mode is not functioning while using Cluster on the nSA.
1350376	Configuration sync not working with SNMP configuration.
22.7R1.2	

Problem Report	Description
PZT-42809	Gateway status constantly changes from not ready to ready on the nSA platform.
PZT-43215	Issue in decoding entity-ID while uploading config to nSA.
PZT-44321	Readiness failures observed in Gateway.
PZT-44342	Config sync rule on the nSA shows Failed and Pending status.
PZT-44990	Issues with Tenant Creation when subdomain has . (DOT) via MSP Portal.
PZT-45039	Performance statistics and other graphs are not visible on nSA.
PZT-45037	SNMP trap messages under Event log to be removed.
PZT-44226	License seat utilization remains constant at 273 users on nSA.
PZT-44225	Analytics data is not populated on nSA Dashboards.
PZT-44103	Single node cluster to support config sync and Report generation.
PZT-43989	nZTA messages can to be more descriptive.
22.7R1	
PZT-44896	ICS Gateway Packages Release Date shown is incorrect under Installation Packages.
PZT-44862	License Subscription expired message shown for user with Active subscription.
PZT-44311	Gateway connectivity issues and the intermittent log uploading issue seen with nSA.
PZT-44103	Config synchronization and Report Generation issue with Single Node cluster.

Problem Report	Description
9.1R18.5/22.6R2.3 (ICS GW)	
PZT-43145	When the client connection set was chosen, certificates were indicated as dependencies.
PZT-43104	Event Log Issues related to external syslog server connection reset.
PZT-43095	Gateway is in nSA licensing mode but unable to connect to Ivanti Neurons for Secure Access' to fetch user license
PZT-43035	The new user registration process should dispatch the authentication URL instead of the enrollment URL.
PZT-42338	The configuration upload to nSA or Pulse one will be initiated again incase there are additional users logging in. If there are constant new users logging in, the full configuration upload will take longer.
PZT-41970	Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI.
PZT-41961	Config sync push fails if /configuration/system/maintenance/options/gro-on-off is selected.
PZT-42809	Gateway status constantly changes from not ready to ready on the nSA platform.
PZT-41472	The status of the configuration synchronization template is stuck in the Pending state.
PZT-43133	Number of Users exceeds Realm Capacity error seen with nSA Licensing Mode enabled.
22.6R1.2	
PZT-37841	Report format CSV/JSON has the epoch timestamp instead of human readable.

Problem Report	Description
PZT-42285	Incorrect selected user roles displayed for Split tunneling policies.
PZT-42378	Peer SP configurations are not getting uploaded to nSA with appropriate title.
PZT-42049	Gateway information not being synced with nSA on 22.5R2.1 version.
PZT-41931	ICS is synchronizing users in Auth Servers to Pulse One.
PZT-41850	ICS Gateway (Event, Admin and user access) Logs are not seen in nSA controller.
PZT-41637/PZT-41354	HTTP error 500 after PUT and Unknown errors in Gateway Events Access logs
PZT-41535	Config sync rule on the nSA shows Failed and Pending status.
PZT-42012	Unsupported attribute type 0' errors in Gateway Admin Access logs during config sync operation
PZT-41970	Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI.
22.6R1	
PZT-41418	nSA Subscription users page is not listing users when the number of reserved license seats are more than 20K. Pagination is now added on User Table UI page along with new UX table changes.
PZT-41470	SAML authentication server configuration with incorrect values.
PZT-41471	Configuration changes made through the nSA UI to the ‘source’ gateway do not reflect or have a very long delay in being reflected in Multinode Config Synchronization templates.

Problem Report	Description
PZT-41473	Incorrect selected user roles displayed for Split tunneling policies.
PZT-41334	Pagination not working with user roles in nSA.
PZT-40864	nSA Reports: Dropdown shows max 100 options (all dropdowns).
PZT-38774	When multiple client packages are present in gateway, errors are seen while uploading configurations to nSA.
PZT-36639	ICS not sending logs to nSA and sessions are not reported.
22.5R1.3	
PZT- 41484	Data is not loading under Insight > Applications.
22.5R1.2	
PZT-41074	Upload ESAP Packages issue on nSA is fixed.
PZT-40843	Fixed log swap issue between the gateway and timestamp fields
22.5R2.1 (ICS GW)	
PZT-40795	As part of logs optimization, Optimized (reduced) the number of API calls triggered from gateways to controller.
PZT-40794	As part of logs optimization, Optimized the critical log message in Gateway Readiness API calls from gateways.
PZT-40730	As part of logs optimization, fixed Gateway getting disconnected and connection error due to SSL read error log messages.
PZT-40706	Fixed issue where sometimes Config upload was triggered quite frequently with no config change done on the gateway.

Problem Report	Description
PZT-40843	Log swap issue, where Gateway and Timestamp fields are interchanged after line #1001 is fixed.
22.5R1	
PZT-40361	ICS is shown as Default upon first login after tenant creation.
PZT-40068	When Terminal Service Profile had special characters the config upload fails.
PZT-38883/38860	Log enhancements in event logs for failure cases.
22.4R2.1 (ICS GW)	
PZT-39635	Program unityConfigSpli fails after gateway reboot and config upload.
PZT-39366	Program jsonConfigHelpe failed, error message is displayed during cofig upload.
22.4R2	
PZT-38102	Program failed after upgrading to latest 22.4R2 builds.
22.4R1	
PZT-38859	Unable to create terminal services profile from nSA
PZT-37709	Pushing full configuration to blank target does not happen.
PZT-38837	Entire config sync is failing with 'Node 'bookmark' identifier count mismatch' error.
PZT-38827	Trying to modify configurations on ICS through nSA Interface, then you have to submit the configuration change multiple times.
22.3R1	
PZT-33001	Config template: SAML settings XML import fails if FQDN is not configured.

Problem Report	Description
PZT-32924	Config Synchronization fails with error.
PCS-36871	Configuration upload is not happening after rebooting the Gateway from nSA.
PZT-33341	Config Template: Adding local auth server for 22.1R1 template fails.
PZT-33708	During Config Synchronization operation, you see 'The system log file is corrupt. Contact Support immediately entry in GW Admin access logs.
PCS-36976	Device attribute is not present in role mapping when MDM server is used for device attribute.
PZT-33343	On cluster nodes Network > Overview, Port status may appear as incorrect such as blank, Not connected.
PCS-35938	Once Client package download starts from nSA to ICS Gateway, any other operations in nSA (For example, Role/Realm creation, any config modification)
PCS-36969	"Add to all VLAN route tables" option is not present in nSA.
PCS-36971	Mac address and link local address are not present for internal/external/management port in nSA.
PCS-36720	TOTP User status is shown as Unlocked, even after unlocking from nSA.
PCS-36747	Role name not present in "Applies to Role" for any Auto Resource policies.
PCS-36757	Internal server error is observed while deleting the user roles.
PZT-32806	Delay in creating User roles from nSA.
PZT-31534	Gateways are not getting listed in nSA after deleting and re-registered.

Problem Report	Description
PZT-31512	The edit name functionality for SAML Authentication server is not working.
PCS-36700	Binary User configuration file import not supported from nSA for file size above 300 MB.
PZT-32799	Unable to delete multiple sign-in URLs on a gateway.
PCS-35403	Test Enrollment is not working in Enterprise Onboarding.
PZT-31275	'Enable periodic password change of machine account' text-box value of AD server is not getting updated/pushed to Gateway from nSA.
PZT-31693	The status of 9.x Gateway in A/P cluster is shown incorrect in nSA, even though they are online and both notification channel and registration.
PCS-34028	Logs not related to configuration done from configuration template is visible under Config Template > Logs.
PZT-29269	The configuration is not pushed to the Gateway, when adding a disconnected state Gateway to the configuration template.
22.2R1	
PZT-29298	nSA UI must indicate to Admin if the template configuration is modified using Gateway Admin UI.
PCS-33427	Test Connection to LDAP and Remote TOTP authservers fail, when executed from nSA UI.
PZT-29259	When invalid file (.rec) is uploaded while creating ACE server, which affects the entire config group management feature.
PCS-33546	Activated/Default Ivanti Secure Access Client package details are not displayed in nSA.

Problem Report	Description
PCS-33308	Ivanti Secure Access Client > Components page in nSA displays different client package versions details when compared with ICS Gateway.
PCS-33633	The Trusted Server List popup is displayed incorrectly.
PCS-33873	Entity ID is not fetched for SAML metadata provider settings.
PCS-33881	User Role fails to push to Gateway with NFS file attribute errors.
PCS-33394	UI issues observed in Always On VPN wizard.
PCS-33859	Unable to download the MIB file in SNMP tab in log settings.
PCS-33219	Post Registration and during config upload, authentication realms admin related logs printed in Gateway event logs.
PCS-33268	Test Connection functionality in MDM Auth Server is not working properly in the Gateway.
PCS-34214	IP address configuration getting pushed from nSA to Gateway but not visible in nSA.
PCS-34122	Not able to create any type of MDM Auth Server.
PCS-33486	Search option is not available in users list for system local auth server.
PCS-34233	Internal server error is displayed when user realm configured from nSA with multiple Auth servers.
PCS-31552	Under the code signing page, delete certificates functionality is not working properly.
PCS-33407	"Not found" error is seen on Hostchecker options page when connection control policy is not configured.

Problem Report	Description
22.1R1	
PZT-27718	View All link from the "Gateways Access Trend chart" from Insights > Gateways page, shows incorrect total rows count on the table.
PCS-31198	Adding a Gateway to a cluster in GW UI does not add the cluster as a group on nSA.
PCS-32081	nSA shows L4 connection as WSAM instead of PSAM connection.
PCS-30330	Cluster is not deleted from nSA on deleting the same cluster from Gateway UI.
PCS-32923	User can see same Host Checker (HC) policy with multiple entries (one with space and the other without) on the Gateway Overview page.
PCS-31061	nSA shows "Gateway status not ready" due to an error encountered in ICS.
PCS-31164	When HTML5 bookmark backend resource is not reachable from the Gateway, nSA insights doesn't show the HTML5 bookmark access details.
PCS-31139	9.x PCS: When the user opens internal directories/files for a particular file bookmark of 9.x, an additional active application count is observed on nSA.
PCS-31232	Default "Meeting Sign-In Page" is missing at "Authentication > Signing In > Sign-In Pages" on VMware VM in 9.12.
PCS-31169	9.x PCS: WELF filter is missing in the filters section, and two JSON filters are present.
PCS-31229	Unable to create Resource profile file of type Unix.

Problem Report	Description
PCS-31230	Default welcome banner shows up the text "Connect Secure" when upgraded from version 9.1R12-14139 to 9.1R12-15707.
PZT-25667	ICS Gateway: The source IP of an end-user session is sometimes seen as 127.0.0.1 under Insights.
PCS-31180	9.x PCS: The Telnet/SSH application count is coming as 0 on the nSA.

Known Issues

The following table describes the open issues with workarounds where applicable.

Problem Report	Description
22.8R1.2	
1567051	**Symptom**: Start time may appear as blank for cluster which are part of config sync rule, when cluster status is not yet synced with controller **Workaround**: Wait for cluster status sync to happen with controller or DIsable/Enable cluster nodes, then trigger config sync rule
1567060	**Symptom**: Eligible Gateways count shows extra entries when 9.X GW's are also registered with controller. **Workaround**: N/A
1567057	**Symptom**: Sequential stage and upgrade for the valid gateways also fails with a toast message in UI even when there are multiple standalone gateways/cluster triggered for stage and upgrade does not meet the criteria for the gateway version not supported/gateway disconnected **Workaround**: NA
1567056	**Symptom**: Toast message in the UI shows the gateway id instead of gateway name when there is a failure in triggering stage/upgrade which could happen due to the gateway version not supported for stage/upgrade or if the gateway is in disconnected state **Workaround** : NA
1567055	**Symptom**: Gateway List page will show the status of a specific gateway as "4/4 Upgraded" instead of "4/4 Staged" once the package is staged successfully on the gateway **Workaround**: NA
1555895	**Symptom**: INSTALL button post successful staging will still be visible in the UI under Manual/Schedule Stage and Upgrade tab even when GW upgrade is already in progress **Workaround** : NA
1537917	**Symptom**: Screen flickering issue seen sometimes during the execution of a config sync rule. **Workaround**: Navigate to any other page and come back to config sync page

Problem Report	Description
1566820	**Symptom**: Restarting services fails to update or synchronize the cluster status on the controller. **Workaround**: Disable/Enable node will sync cluster configuration on nSA.
1564363	**Symptom**: Unable to modify Custom Expression from nSA. **Workaround**: NA
1565991	**Symptom**: McAfeeAntiVirusHigh default AV import issue. **Workaround**: • Unmap default McAfeeAntivirushigh device policy in auth policy or in secure access policy if configuration import error in Admin logs or warning in device policy page. • Create custom AV policy for McAfeeAntiVirusHigh and map it for the policy.
1553286	**Symptom**: Syslog forwarding configuration with "via Gateways" on ZTA may impact syslog forwarding for nSA and ZTA. **Cause**: System tries to forward logs "via Controller" also even with configuration "via Gateways" on ZTA. **Workaround**: On ZTA, Configure Syslog Server for ZTA "via Controller" only.
1441152	**Symptom**: TCP dump action under Gateway Troubleshooting in nSA/ZTA fails to upload the dump to Troubleshooting overview intermittently when admin is unable to stop the TCP dump **Workaround**: TCP dump could be available from ICS Gateway console and in case of ZTA, re-try triggering TCP dump action
1546793	**Symptom**: Unicodes are seen sometimes in the Tenant UI instead of Icons. **Condition**: While using the Tenant using Chromium browser. **Workaround**: No functional impact. Reopen the App in another tab in the browser, issue will not be seen.
22.8R1	
1525838	**Symptom**: When source gateway is running on version 22.7R2.5 or lower and target gateway is running on version 22.7R2.6, during selective config sync operation, config sync gateway status remains in Importing state.

Problem Report	Description
	Workaround: Include at least one modified configuration option from Systems Settings > Configuration in the config sync rule when the source gateway is running version 22.7R2.5 or lower and syncing to a target gateway running version 22.7R2.6 Or Upgrade source gateway to version 22.7R2.6.
1512871	**Symptom**: Config Sync Schedule Jobs - creating schedule job with no end date results in an unknown error. **Workaround**: Create schedule job with some end date, then edit rule, and set date to no end date.
1512873	**Symptom**: Report job fails when creating a report adhoc or scheduled, and an admin configures it to share with any admin user in the tenant. **Workaround** : NA
22.7R1.6	
1432490	**Symptom**: Admin can observe Active Session count mismatch between Gateway and nSA Dashboard intermittently. **Workaround**: Session count is synced hourly. Admin should see matched count every hour.
1474106	**Symptom**: GroupBy option in tenant admin logs is not showing any data. **Workaround**: No workaround.
1473258	**Symptom**: Config Sync Status shows an error. **Workaround**: No workaround, see Config Sync Rule.
1440328	**Symptom**: TCP dump action under Gateway Troubleshooting in nSA/ZTA fails to upload the dump to Troubleshooting overview intermittently when admin is unable to stop the TCP dump **Workaround**: TCP dump could be available from ICS Gateway console and in case of ZTA, re-try triggering TCP dump action
22.7R2.3 (ICS GW)	
1438777	**Symptom**: jsonConfigHelpe process crash is observed during config sync operation. **Condition**: When entire config sync operation failed with long error message, splitted failure. log messages got truncated, due to which sometime jsonConfigHelpe process crash is observed.

Problem Report	Description
	Workaround: Try Selective config sync.
1438986	**Symptom**: XML Import failure logs gets truncated on Gateway during config sync operation. **Condition**: When entire config sync operation failed with long error message, splitted failure log messages got truncated. **Workaround**: Try Selective config sync.
22.7R1.5	
1442614	**Symptom**: Error while trying to reset TOTP user account from nSA controller under Administration > Admin Management > Authentication Servers if secondary auth is configured for the sign-in policy **Workaround**: No workaround
1440328	**Symptom**: TCP dump action under Gateway Troubleshooting in nSA fails to upload the dump to Troubleshooting overview. This issue happens intermittently when Admin is unable to stop the TCP dump. **Workaround**: Use the ICS Gateway console for performing the TCP dump.
22.7R1.4	
1410360	**Symptom** : The consolidated landing page (ZTA+nSA) is currently in preview mode, you may see some discrepancies between the chart counts and the logs/table views of the corresponding charts. **Workaround** : No workaround
1416259	**Symptom**: The platform license fails to update in the gateway after toggling between gateway license and nSA licensing modes. **Condition**: Post-transition from the default Gateway licensing mode to nSA named user licensing mode, login is restricted to more than two users. **Workaround**: Restart the services or reboot the gateway.
1415021	**Symptom** : Column re-sizing is not supported under Administration > Subscriptions > Users **Workaround** : No workaround
22.7R1.3	

Problem Report	Description
1390038	**Symptom**: In certain cases, incorrect tenant identity values are included in messages transmitted by Gateways that are registered with the nSA Controller. This may cause the controller to overlook certain log messages and cause the related data to disappear from analytics dashboards. **Workaround**: No workaround
1350117	**Symptom**: nSA Config Sync: The admin log for the sync rule is not appearing. **Workaround**: No workaround
1350201	**Symptom**: When exporting logs for any L4 dashboard, the active view data is displayed for the previous four days, but only the last hour is exported. **Workaround**: To see the correct logs in a csv or json export, choose the custom time range that needs to be sent with the data.
1370506	**Symptom**: Active view (past 1 hour): The home page for nSA+ZTA's consolidated data will only display the current user count activity, not the entire history of user activity over the previous hour. **Workaround**: ZTA users' total activity over the past hour (Active view) will be displayed on the Overview page.
1389307	**Symptom**: The All Gateway count on the Overview page and Insight > Gateways summary shows the registered and online gateways count only in the historic view. **Workaround** : No workaround
1391196	**Symptom**: Username sorting is not working on Subscriptions > Users page **Condition**: Observed when subscription page has entries without username, only device login entries. **Workaround**: No workaround
1391320	**Symptom**: Offline Gateway count doesn't gets displayed on Gateway Overview page. **Condition**: This is observed with certain screen resolution. **Workaround**: Increase screen resolution to fix the issue.
1391819 -	**Symptom**: Any number of nodes can be added while creating cluster from nSA. **Condition**: For Gateways other then virtual Gateways. **Workaround**: No workaround

Problem Report	Description
1392074	**Symptom**: Unable to login to staging tenant, getting 'Your request could not be authenticated (Error 401)'. **Workaround**: Relaunch the browser or login using incognito mode.
1392173	**Symptom**: Error message while upgrading cluster from nSA when its status is not yet updated. **Workaround**: No workaround
1391936	**Symptom**: On the Consolidated Landing Page, the Current Day view (Displayed as Last X hours) may show a count mismatch between the Summary Panel and the Table. **Condition**: When admin wants to view details of current day's data. **Workaround**: The admin can utilise the custom view to observe data for the same time range.
1391923	**Symptom**: The admin might notice discrepancies between the device counts in the Summary Panel and the Table view when clicking on the counter. **Condition**: Endpoints without a device identification number or share the same device identification number. **Workaround**: Consider the Summary Panel count as the accurate count.
1345443	**Symptom**: Even after turning off the proxy, ICS keeps using it to communicate with the nSA (notification channel). **Workaround**: Reboot the ICS Gateway when there is a change in Proxy setting.
1375541	**Symptom**: With gateways upgraded from 9.1R18.2 to 9.1R18.6 and higher, config sync has known issues with maintenance/archiving settings. **Workaround**: If archive system configuration or archive user accounts is enabled then update day settings may be blank after upgrade then save these settings from nSA UI and retrigger the config sync rule.
1393588	**Symptom**: After upgrading the Gateway from nSA, nSA continues to show the previous version/unupdated version. **Workaround**: Restart the services/Restart the Gateway.
1393779	**Symptom**: 1. Invalid download URL error while importing ESAP package. 2. Not Found error while browser HC policies. **Condition**: 1. Whenever custom ESAP package is uploaded from nSA UI, 'Invalid Download URL' error is seen.

Problem Report	Description
	2. After successful activation of the custom ESAP package on Gateway, a Not Found error prevents the Host Checker (HC) Create Read Update Delete (CRUD) operations from being completed from the nSA UI. **Workaround**: Perform HC policy CRUD operations from the Gateway UI.
1393374	**Symptom**: The count shown for specific gateway version might differ between the Gateway by version chart and the table view under Insights > Gateways in nSA. **Workaround** : No workaround
1393507	**Symptom** : Consolidating landing page(ZTA+nSA) is in preview mode and hence there could be data mismatch between the counts on the chart compared to the logs/table view of corresponding charts. **Workaround** : No workaround
1393980	**Symptom**: If admin activates an unsupported ESAP package on the nSA Controller UI, it results in deletion of all the existing ESAP packages from the gateway. **Condition**: Admin activating an unsupported ESAP package on the nSA controller UI. **Workaround**: Admin can activate a supported ESAP package from nSA or from the Gateway UI. For minimum supported ESAP version, refer to Supported Platform Guide.
1393596	**Symptom**: Admins might observe a slight difference in the CPU, Swap Memory, Disk Usage and Network Throughput values shown on the tooltip forTop Gateways by Health chart under nSA > Insight > Gateways and the table view logs for respective gateways. **Workaround** : No workaround
1393991	**Symptom**: Read only admin is able to make changes to cluster status and properties on nSA controller UI. **Condition**: Read only admin performing CRUD operations of cluster status and properties on nSA controller UI. **Workaround**: No workaround
1375541 1410472 1397661	**Symptom**: Selective config sync with archiving settings or entire config sync failure.

Problem Report	Description
	Condition: Selective config sync of 'archiving' settings or entire config sync may fail with could not access or modify schedule item in cache or component selected without selecting any Day error. **Workaround**: Either remove archiving settings from config sync rule or fix components where days are not selected.
1397639	**Symptom**: Selective config sync with automatic snapshot settings or entire config sync failure. **Condition**:Selective config sync of automatic snapshot settings or entire config sync may fail with Take a snapshot every (minutes)] Invalid value 0: integer must be 1 to 20219 error. **Workaround**: Either remove automatic snapshot settings from config sync rule or fix snapshot settings.
1401676	**Symptom**: Selective config sync with 'User Realms' settings or entire config sync failure. **Workaround**: Remove 'User Realms' settings from config sync rule.
1401674	**Symptom**: Selective config sync with Certificates settings or entire config sync failure. **Condition**: Selective config sync of 'Certificates' settings or entire config sync may fail with Invalid reference error. **Workaround**: Remove Certificates settings from config sync rule or manually import the certificate which is causing failure.
1401671	**Symptom**: Selective config sync with Security settings or entire config sync failure. **Condition**: Selective config sync of Security settings or entire config sync may fail with Custom cipher does not match the available selection error. **Workaround**: Remove Security settings from config sync rule or manually change custom chiper which is causing failure.
1408888	**Symptom**: Selective config sync with Certificates settings or entire config sync failure. **Condition**: Selective config sync of Certificates settings or entire config sync may fail with Invalid value for node crl-download-frequency error. **Workaround**: Remove Certificates settings from config sync rule or manually change crl-download-frequency for certificates which is causing failure.

Problem Report	Description
1408889	**Symptom**: Selective config sync with PSAM destination profile settings or entire config sync failure. **Condition**: Selective config sync of PSAM destination profile settings or entire config sync may fail with Invalid value for identifier destination error. **Workaround**: Remove PSAM destination profile settings from config sync rule or manually fix PSAM destination resource entries which is causing failure
1397914	**Symptom**: Selective config sync with Log/Monitoring settings or entire config sync failure. **Condition**: Selective config sync of Log/Monitoring settings or entire config sync may fail with Modification of this attribute is not allowed error. **Workaround**: Remove Log/Monitoring profile settings from config sync rule or manually fix attribute entries which is causing failure.
1397916	**Symptom**: Selective config sync with Admin Roles settings or entire config sync failure **Condition**: Selective config sync of Admin Roles settings or entire config sync may fail with Invalid IP Address error **Workaround**: Remove Admin Roles settings from config sync rule or manually fix IP entries which are causing failure.
1393598	**Symptom**: Selective config sync with Logs/Monitoring settings or entire config sync failure **Condition**: Selective config sync of Logs/Monitoring settings or entire config sync may fail with error **Workaround**: Remove Logs/Monitoring settings from config sync rule or manually fix log size below 200 MB which is causing failure.
1414913	**Symptom**: Selective config sync with SAML auth server settings or entire config sync failure. **Condition**: Selective config sync of SAML auth server settings or entire config sync may fail with 'soap-responder-url is non-empty and source-id is empty' error. **Workaround**: Remove SAML auth server settings from config sync rule or manually fix soap-responder-url and source-id field entries which is causing failure.
1408890	**Symptom**: During Gateway rollback observing, 'Failed to upload configuration commit message; Transfer returned result code 56' errors in Event logs.

Problem Report	Description
	Workaround: No workaround. Config upload works in the subsequent attempt.
22.7R2 (ICS Gateway)	
PZT-45021	**Symptom**: TCP Dump size is 0 when captured from nSA. **Condition**: Capture TCP Dump from nSA and verfiy its size. **Workaround**: Capture TCP Dump from ICS Gateway.
22.6R1.2	
PZT-42338	**Symptom**: The configuration upload to nSA or Pulse one will be initiated again incase there are additional users logging in. If there are constant new users logging in, the full configuration upload will take longer. **Workaround**: None
22.6R1	
PZT-41640	**Symptom**: SAML dependencies check does not include all checks, while creating the config sync rule. **Condition**: When any configuration is dependent on the SAML Auth server, whether it is being used as a service provider or identity provider. **Workaround**: Manually select all the SAML dependencies.
PZT-41354	**Symptom**: HTTP error 500 after PUT and Unknown errors in Gateway Events Access logs **Condition**: Observed during Gateway rollback. **Workaround**: No functional impact. Config upload works fine upon retrying.
PZT-42049	**Symptom**: Analytics Dashboard and Gateway logs are not synced with nSA. **Condition**: ICS Gateways running on cloud with version 22.5R2 or above. **Workaround**: NA
PZT-42012	**Symptom**: 'Unsupported attribute type 0' errors in Gateway Admin Access logs during config sync operation. **Condition**: Observed when config sync operation is performed where source gateway is running on R1 build (FIPS) and target gateway is running R2 build (Non FIPS) **Workaround**: Exclude security settings from config sync rule.
PZT-41970	**Symptom**: Config rule push status for the failed gateway will be in "pending" state in nSA Admin UI.

Problem Report	Description
	Condition: Config sync rule might fail for one of the target gateways, if entire config sync is pushed to multiple gateways. **Workaround**: Delete the failed gateway entry from the config rule and create new config rule for the failed gateway only.
PZT-41961	**Symptom**: Config sync push fails if /configuration/system/maintenance/options/gro-on-off is selected. **Condition**: This issue can be seen for both Hardware appliances as well Virtual appliances. **Workaround**: Avoid selecting this option while creating a config sync rule.
22.5R1	
PZT-40105	**Symptom**: Dependency check for resources policies. **Condition**: When resource policies are part of config sync rule. **Workaround**: Do not include resource policies in selective config sync rule or skip dependency check.
PZT-40644	**Symptom**: HTTP PUT errors observed in logs. **Condition**: When Gateway is registered with nSA sometimes HTTP put errors observed in Events logs. **Workaround**: NA
22.4R3	
PZT-39636	**Symptom**: When RBAC user navigates to Config Sync rule page, you may not see config sync rules properly. **Condition**: While creating RBAC role with connect secure Gateway permissions, user does not select GW's under selected Gateways list which are part of Config Sync rule. **Workaround**: Make sure to select all GW's under selected Gateways which are part of config sync rule while creating RBAC role.
22.4R2	
PZT-39635	**Symptom**: Program unityConfigSpli fails after gateway reboot. **Condition**: When gateway is registered with nSA and upon gateway reboot. **Workaround**: NA
22.4R1	

Problem Report	Description
PZT-39310	**Symptom**: Config upload post Gateway reboot fails when configurations with resource profile name containing unicode characters. For example but not limited to : ¯, ß, ð, ƒ, ©, þ. **Workaround**: Identify the unicode characters in resource profile and remove them from gateway.
PZT-38809	**Symptom**: Admin may not find all application names in the sanky chart which are listed in the access trend chart. **Workaround**:NA
PZT-38806	**Symptom**: Admin may see some text and labels in lower case and some in upper case **Workaround**: NA
PZT-38774	**Symptom**: When multiple client packages are present in gateway, errors are seen while uploading configurations to nSA. **Workaround**: It is recommended to have only one client package in Gateway.
PZT-38670	**Symptom**: Binary config import from a Gateway, which is registered to a different nSA, client certificates are getting replaced. After the import is successful, as the client certificates are getting replaced GW is trying to communicate to a different nSA due to which GW is going to "not ready" state. **Workaround**: After the binary configuration import is successful, we need to remove the client certificates and re-register the GW.
PZT-38714	**Symptom**: If one of the gateways goes down in a cluster, nSA is not showing the active session with another gateway, it still shows connected with the gateway which is down. **Workaround**: NA
22.3R4	
PCS-39826	**Symptom**: Failure logs are seen multiple times during config sync operation. **Condition**: When config sync rule fails, it is observed that failure logs are seen multiple times. **Workaround**: Skip configuration, which is failing from config sync rule and trigger same rule again.
22.3R1	
PZT-33008	**Symptom**: Uploaded device certificate is not visible on the nSA.

Problem Report	Description
	Condition: When using nSA to import device certificate onto the ICS gateway. **Workaround**: Wait for at least 10 seconds, and then refresh the page.
PZT-36639	**Symptom**: ICS not sending logs to nSA and sessions are not reported. **Condition**: When Admin configures the JSON filter. **Workaround**: Remove JSON filter, which was created manually.
PCS-39623	**Symptom**: Upgrade of cluster node fails with "Unable to extract installer" error message. **Condition**: When upgrade triggered on a cluster: • Node-1 upgrades successfully to 22.3R1 and prompts Node-2 to upgrade. • Node-2 copies the package from Node-1, but fails to extract the installer. • This is due to free disk space constraints on Node-2. **Workaround**: Follow the below procedure: 1. Power cycle Node-2. 2. Press Tab and boot into Standalone mode. 3. Access the UI and follow the procedure mentioned in https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44877/?kA13Z000000L3Z5 to clean up space. 4. Reboot and join the cluster. Upgrade should now go through fine.
22.2R1	
PCS-36834	**Symptom**: Radius Auth server User Attributes do not display code/number associated with them on nSA UI. **Condition**: Creating/Editing a Role Mapping rule based on User Attributes under a User Realm with Radius auth server. **Workaround**: The code/number associated with the attributes can be viewed on GW UI.
PCS-36937	**Symptom**: Enduser is not able to receive multicast traffic. **Condition**: When the enduser is connected to VPN in ESP. **Workaround**: Not applicable

Problem Report	Description
PZT-33361	**Symptom**: Config Template: Adding MDM server for 22.1R1 template fails. **Condition**: When Admin tries to add an MDM server for 22.1R1 template it shows this element is not expected. **Workaround**: Upgrade the Gateways to 22.2R1 and add this Gateway to 22.2R1 template and create the configuration.
PZT-32568	**Symptom**: Configuration values in Security Settings > Miscellaneous page is not retained. **Condition**: When nSA admin tries to configure values in Security Settings > Miscellaneous page. **Workaround**: No functionality impact, configs are pushed successfully.
PZT-33401	**Symptom**: Second node in the cluster is shown as disconnected. **Condition**: Upgrade from older release to 22.2R1 build, through nSA. **Workaround**: Navigate to the cluster through nSA and check the status.
PCS-36458	**Symptom**: Default and Factory version name is not displayed for default Ivanti Secure Access Client package. **Condition**: Admin selects the gateway and accesses Ivanti Secure Access Client Components. **Workaround**: Not applicable
PCS-34681	**Symptom**: Roll back option not available in nSA for AA cluster. **Condition**: When Admin tries to do a roll back from nSA. **Workaround**: Reboot the AA cluster.
PCS-36458	**Symptom**: Default and Factory Version labeling name is not displayed for default Client package. **Condition**: Select gateway and access Client Components in nSA. **Workaround**: Not applicable
PCS-34067	**Symptom**: Resource not exists is displayed while trying to delete Internal, external, management port. **Condition**: Select a gateway > Navigate to Network > Vlan > Internal, external, management > virtual port. **Workaround**: Perform the Configuration using Gateway Admin UI.
PCS-36695	**Symptom**: Unable to configure cluster when License server configured on both nodes.

Problem Report	Description
	Condition: When License server is configured on Gateways used to create cluster. **Workaround**: Remove License server configuration from Gateways and create cluster.
PZT-32537	**Symptom**: When admin tries to filter out logs in Template> logs page. **Condition**: When controller logs filter is set to true. **Workaround**: None
PZT-32981	**Symptom**: XML Import of SAML SSO 1.1 policy and creation from nSA fails. **Condition**: Import of SAML SSO 1.1 policy and policy creation. **Workaround**: Use the Gateway Admin UI.
PZT-32749	**Symptom**: "Unknown Error" is displayed on the nSA Admin UI, while adding gateway to configuration template. **Condition**: When admin tries to add gateway with many large configurations. For example, many Host Checker policies. **Workaround**: Ignore the error as the Gateway is added to template and config is pushed to gateway.
PZT-31008	**Symptom**: Expired certificate is getting imported on nSA from Config Template > Trusted Server page. **Condition**: When Admin tries to import an expired CA certificate in nSA. **Workaround**: Ensure that the certificate is valid before importing it on nSA.
PZT-30913	**Symptom**: Editing the configuration name is not working on nSA. **Condition**: Create an new component set for Client Components, edit the name of the component set and the edited name is not being reflected in nSA but it is successfully pushed to ICS Gateway. **Workaround**: No functionality impact.
PZT-31638	**Symptom**: Updating ESAP package to cluster will not work when one node is in connected state and other is in disconnected state. **Condition**: When user tries to update the ESAP package to a cluster. **Workaround**: Update ESAP package from the active node configuration.
PZT-29300	**Symptom**: Reconcile configuration takes few seconds. **Condition**: Select a Gateway or cluster, which exists in the configuration template and click Reconcile configuration. **Workaround**: None

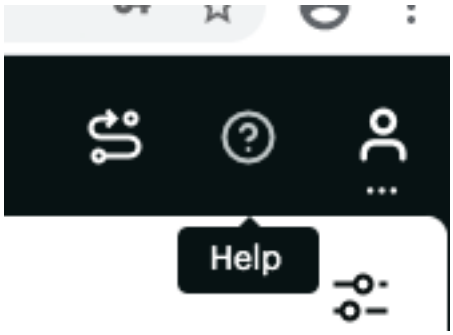
Problem Report	Description
PZT-29049	**Symptom**: Deletion time is high while deleting the config in configuration template. **Condition**: Deleting many server configurations at a time. **Workaround**: Deleting minimal amount of configuration or server config from template.
PCS-33870	**Symptom**: File upload fails to push to Gateway for VMware and Citrix download configurations. **Condition**: Admin tries to upload large size file. **Workaround**: Use the Gateway Admin console to upload the configuration.
PCS-36464	**Symptom**: ICS gateway model details not updated correctly on nSA. **Condition**: When licenses are installed on Gateway after nSA registration. **Workaround**: Install all required licenses before registering to nSA.
PZT-33115	**Symptom**: Deleting AD Auth server shows internal server error in nSA. **Condition**: Deleting AD Auth server from nSA. **Workaround**: Refreshing the page shows AD AUTH is deleted.

Limitations

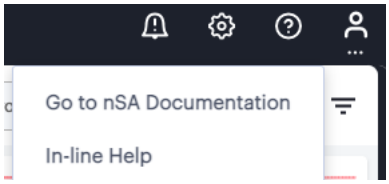
- Cluster is formed with only one node while creating from nSA when license server is configured on one of the nodes.
- The nSA Controller does not support the use of the "/" character for configuring sign-in notifications on ICS. This limitation applies to the sign-in URL, authentication server creation, and other relevant settings across all nSA user interface pages, including characters such as: #, ?, /, \, %.
- After importing the binary configuration in ICS Gateway, you must re-register the Gateway with nSA. For reregistration, see Tenant Admin Guide.
- RBAC: If the tenant has both nSA and ZTA gateway, setting any common permissions while creating an Custom RBAC Admin Role applies to both nSA and ZTA gateway. For example, if custom admin role has modify permission for ZTA gateway then the same applies to nSA gateway also.
- The ICS upgrade time from nSA depends on the network bandwidth and latency. If the downloading of package takes more than 4 hours then the upgrade process is marked as failed.
- Cluster creation from nSA takes few minutes to create cluster and Add/Join members.
- The time taken for Config Synchronization process from source to target Gateway depends on the configuration size.

Documentation and Technical Support

nSA documentation for administrators is available from the Tenant Admin portal. If you are an administrator, login to the portal using the URL provided in your welcome email after setting up your product subscription. To access product help and documentation links, click the "?" help icon in the navigation bar:



From the drop-down list of Help options, click "Go to NZTA Documentation":



To access nSA documentation, you must be logged in to the Tenant Admin portal.

For other Ivanti products, documentation is available at https://help.ivanti.com/

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to https://help.ivanti.com/. Find CSC offerings: https://forums.ivanti.com/s/contactsupport

Technical Support

When you need additional information or assistance, you can contact Technical Support:

- https://forums.ivanti.com/s/contactsupport
- support@ivanti.com